SEB SECURITY

GENERAL INFORMATION

- Prevent any unfair advantage of one company over any others.
- Prevent any conflict of interest or appearance of conflict of interest.
- Minimize any pressure on personnel serving on the evaluation panel.
- Access to information is limited on a need-to-know basis to personnel listed on the Appointment Memos. Supervisors not directly involved may contact the Chairperson for any information they might need.

GENERAL INFORMATION (Continued)

- Outside evaluators may not be used in evaluating proposals unless they are hired as Special Government Employees prior to serving on an SEB (must comply with FAR 37.2 and NFS 1837.2).

- Any calls received with regards to procurement should be reported to Contracting Officer and/or Chairperson.

- May continue to interface with contractors on your current contracts. Do not attempt to answer any questions with regards to SEB activities. Questions should be reported to the Contracting Officer and/or the Chairperson.

PROTECT THE INTEGRITY OF THE SEB PROCESS

SEB SECURITY REQUIREMENTS

1. Physical Security

2. Personnel Security

3. Document Control Security

4. Computer Security

PHYSICAL SECURITY

Access - By one committee at a time

- Only personnel who are involved in the SEB activity may have access to the facility.
- For specific rooms within the complex a sign in/sign out log must be used. The last person leaving the area must ensure5 that all information is secured before leaving.
- Be aware that contractors may work in and visit the building. Make sure that you do not discuss SEB information anywhere but in the SEB room assigned to you. Report any suspicious activities to the SEB Chairperson and Security.
- Routine or emergency maintenance of the SEB area requires that the "uncleared" persons be escorted by a SEB member. No access to activities or information may be allowed.
- Do not discuss SEB sensitive information on the telephone (unless it is a secured phone).

PHYSICAL SECURITY (Continued)

- **MANDATORY** requirement to wear badges at all times

- Keys and/or key cards to the SEB facility
  - Don’t label
  - Report lost keys and/or key cards immediately

- After hours and weekends, notify Security to let them know you are in the SEB facility

ACCESS TO SEB FACILITY MAY BE JEOPARDIZED

PERSONNEL SECURITY

- Clearances required for access to classified information

- Financial statements - after completion, they are returned to Legal. You must disclose ALL financial interests annually.

If at any time you find a possible conflict after initial receipt of proposal, you MUST notify Contracting Officer and/or Chairperson

DOCUMENT CONTROL SECURITY

The following documents are sensitive and shall be controlled:

- RFP before it is released
- Offerors' proposals
- Source Selection - any material received or generated after initial receipt of proposals
- Initial & Final reports
- Presentation charts (including handout copies)
- Committee reports

DOCUMENT CONTROL SECURITY (Continued)

- Protected when not in use. In emergency situations, if possible, lock up information before you exit the area

- SEB-sensitive documents (examples – offerors proposals, source selection information, etc.) should not be removed from or worked on outside of the SEB facility/area, unless approved by the SEB Chairperson and CO.

- All sensitive waste from the SEB must be properly stored until disposal arrangements are made. When cleaning out large amounts of sensitive information, plan ahead…
  - This includes waste from copiers, notes, calculator tapes, and any other sensitive “trash”.

DOCUMENT CONTROL SECURITY (Continued)

- SEB-sensitive documents should be hand-delivered to an individual or, in their absence, to an “SEB cleared” individual.
- SEB-sensitive documents required at HQ should be hand-carried, if possible. If they must be mailed, they must be double-wrapped and sent via “Registered” mail, signed “Return Receipt.”
- SEB-sensitive documents transmitted between Centers should follow classified document procedures.
- All SEB documents distributed in SEB presentations must be returned to the Recorder. It is a good idea to collect them from all personnel (including management) before they leave the presentation room. If individuals need to retain the documents for further action, find out when you should follow up to retrieve the document.

COMPUTER SECURITY

- Computers should not be brought into the SEB Facility; if outside computers are brought into the Facility, they cannot be removed from the SEB Facility until the completion of the SEB and verification is made that they contain NO SEB-sensitive information . Recording devices and cell phones with photo capabilities should not be brought into the SEB facility.
  - Computers located in SEB facilities should never be connected to a network but a stand-alone system
  - Email should never be utilized in communicated SEB sensitive information

VIOLATION/NOTIFICATION PROCEDURE

1. Notification by Security Force Supervisor
2. Incident Report
3. Investigation by Security
4. Report to Management
5. Discussed at Anomaly Review
6. Documented in Final Report
7. Possible Consequence --

YOU START OVER!